Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 4 (2013) 2 – 7

Procedia IERI

www.elsevier.com/locate/procedia

2013 International Conference on Electronic Engineering and Computer Science

The Web Security Password Authentication based the Single-Block Hash Function

Shi-Qi Wang [a], Jing-Ya Wang [a], Yong-Zhen Li[a,*]

[a]*Network & information Security Lab., Dept. of Computer Science & Technology*
Yanbian University, Yanji, China

Abstract

I The paper puts forward the Web security password authentication scheme based on the single-block hash function. The scheme can solve the problem effectively that exists in the traditional password authentication or digital signature in the Web authentication of user's identity to realize the defect. It can resist replay attacks, eavesdropping, modification of messages and common attacks, and low cost, high efficiency, satisfying security and efficient needs of structural features for identifiable authentication in the network service. Generally, MD5 or SHA1 is used. But these algorithms are too cumbersome for the Web authentication of user's identity, and the amount of computation is also too huge. The experimental results show that the scheme guarantees safety at the time, and increases the efficiency of the security authentication.

Keyword: Single-Block Hash Function; authentication ; Web Security; password; message Digest

* Corresponding author. Tel.: +86-0433-2730309; fax: +86-0433-2730309.
E-mail: lyz2008@ybu.edu.cn.

doi:10.1016/j.ieri.2013.11.002

1. Introduction

Due to the rapid development of Internet, people have more and more opportunities to access website security. However, internet environment is treacherous and user's information is easily achieved and copied. Therefore identify of the legitimate users and protecting elusive information of sensitive data are more important. The wide way is to adopt a password to authenticate the identity of a user so far.

Secondly based on the analysis of the Web user's identity authentication[1] and the deficiency of familiar Web authentication scheme, a single-block hash function and practical Web authentication scheme is proposed. The scheme can solve the problem effectively that exists in the traditional password authentication or digital signature in the Web user's identity authentication to realize the defect. It can resist replay attacks, eavesdropping, modification of messages and common attacks, and low cost, high efficiency, satisfying security and efficient needs of structural features for identifiable authentication in the network service [2].

Generally，MD5 or SHA1 is used. But these algorithms are too cumbersome for the characteristics system of Web authentication, and the amount of computation is also too huge. The paper puts forward a single-block hash function designed and the realization of a concrete analysis which analyzes the advantages and disadvantages of its existence. Finally the function is compared and analyzed with MD5 algorithm. The experimental result is improved by using the single-block hash function for website password of user's identify authentication, from the safety , efficiency and so on contrast, to overcome the MD5 algorithm under the condition of insufficient and guarantee the security of authentication.

2. Existing Model of Password based the User's Identity Authentication

User's identity authentication is the process which confirms operator and only identify the user's digital identity in the network. Before the user accesses web site system resources, he must be distinguished by user's identity authentication system firstly, accessing monitor secondly .The system decides whether the user can be able to access the resources [3] according to the user's identity and authorization database. The authorization database let security administrator carry on the configuration in need. Audit system according to the audit setts records the user's request and behavior, and at the same time, the instruction detection system real-time or non real-time detection have invasion behavior. Access control-box audit system is dependent on the user's identity authentication system providing the 'information', called the user's identity.

User's identity authentication can achieve by the following several ways or their combination. The method of the username/password is the most simple and common identity authentication method. In fact because of many users are in order to prevent forgotten the password, they often use password such as their or family's birthday, telephone numbers and easy to be guessed by others, that has many security hidden danger. Therefore the phenomenon is easy to cause the password leak. Even if it can guarantee user password not be leaked, the password is the static data, and in the verification process it needs be transmitted in the computer memory and network, and each time the verification process uses the same validation information. It is easy to stay in the Trojan horse program of computer memory or network of monitoring equipment capture. Smart card authentication mode, each time a user logins the data reading from a smart card, and the data is also static. The technology through the memory scanning or network monitoring technology is easy to intercept to the user's identity authentication information. Biometric authentication [4] mode, such as the user's fingerprint, iris, sounds, etc. Dynamic password authentication technology [5, 6] is a technology of the user's password which changes in accordance with the time or the count of use constantly, each password only is used once. The technology using one password once, effectively ensures the safety of the user identity. But if the Client hardware and Server time or frequency can't keep a good synchronization, it is possible to happen that legitimate users cannot login. When the users login each time, they need input a string of irregular password

through the keyboard. If user inputs one wrong letter, he will input from beginning. The use of the technology is very inconvenient.

Most of the online business is based on the username/password method of the static password identification technology, this way is simple, easy to realize[7,8]. Of course, there are also many hidden security dangers: password easily revealed to others, the password on the internet transmission easily gained, even the credit card numbers, bank numbers, private keys, password and other sensitive information on the network transmission will be stolen by attackers. According to the vulnerability of static password, one-time password concept arises at the historic moment; its main idea is to add password transmission process uncertain factors, making each login authentication information transmission is not same, and replay attacks and impersonation attacks can be avoided.

Based on the static password authentication in hidden security dangers and the insufficiency, this paper puts forward the method based on the single-block hash function for user's identity authentication method. Result of hash function is the abstract of information, its length is usually much smaller than the information, and has a fixed length. Strong encryption of hash function must be irreversible; it means that a result through the hash, it is hard to get the original information. Ensure the user's identity authentication process not to be stolen, intercepted. At the same time it guarantees the security of the password authentication, the balance of efficiency, making it easier to apply for the Web in daily life.

3. Proposed Authentication Protocol

3.1 Single-block hash function algorithm design

Single-Block hash function is a packet length for 128bits, password input and pi of 128–bit irrational for an operation, the output 128bits, each stage with 128 bits and register A, B, C, D as input. Please $A \leftarrow B+(F(B,C,D)+Y[k]+W[i])$ operation, W[i], i[1,16],Y[k] are input data. F、G、H、I are four-stage operation of nonlinear functions [9]. The input character should be controlled in 16 inside, which is within 128 bits. As shown in Fig.1:

Single-Block hash function is grouped by 128 bits to deal with the input information, and each group is divided into four 32-bit son groups, the input value and A, B, C, D constant register for operation, and at the end of stage by stage of preservation before register value to update cache content, the output of the algorithm by four 32-bit group composition, with these four 32-bit packet processing to create A group of 128 bits hash value.

When the four link variables are set up, it begins to enter the algorithm of four-stage stage operation. Stage times are the number of 128-bit information group. Above four link variable copy to four other variables: A to A_1, B to B_1, C to C_1, D to D_1, and so on.

The main circulation has 4 stages; each stage has four times each operation. The operation for A B C and D, three of these as the nonlinear function operation, then the results add the second and fourth variable, and text A child group and A constant to the new result. The new result $<<<s$ stage left s position, and finally the results replaces A.

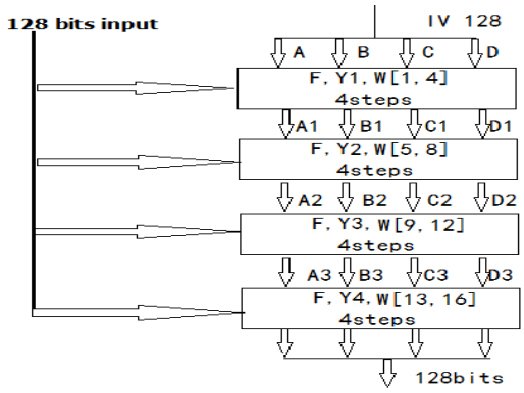

Fig.1 Four-stage structure of main loop

3.2 Web security password authentication process based on single-block hash function

As a result of the use of traditional user name and password to realize Web user's identity authentication exists deficiency, nowadays many researchers research to use Single-Block hash algorithm to realize the Web user ID authentication. The chapter will use the Single-Block hash algorithm to design a new Web password authentication scheme. It will meet the needs of the web user's identity authentication security. And it achieves simply and solves deficiency of the traditional user name-password authentication or digital signature to realize Web user's identity authentication.

1) Godaddy Deluxe:

S: the Server

C: the Client

ID_i: Each user identification number

PW_i: User ID_i corresponding Password

Rs: the Client from the random Number

H(): the Single-Block hash function

2) User Registration:

C→S：ID_i、H$(ID_i+PW_i)=HPW$: User ID_i sends message HPW to the Server to request registration through the safe passageway, PW_i is actual choice for the user password;

C←S：Return to success or not.

The Server receives the user request message, and identity confirmation storage register message$\{ID_i,HPW\}$to the database.

3) Identity Password Authentication

a) Firstly, the Server S saves the user account number and password ID_i, HPW.

b) When a user ID_i hopes to login through the security, the steps are as follows:

c) Call the random number producing function F(Rs), and then return to random number Rs, again after the Single-Block hash function operation, get H$(ID_i+PW_i)=HPW$, calculate H($HPW+Rs$). The message package pack(ID_i,H$(HPW+Rs),Rs$) with the Server to the background Server point.

d) The Server point receive the message package, analysis package, and get ID_i ,H$(HPW+Rs),Rs$; Sending ID_i to find out HPW from the database , compare with H($HPW+Rs$) operation, if the agreement, the authentication success.

4) Change Password:

During password changing stage mainly users need to use a new password *HPW* instead of the old password, denoted HPW_{new}. Probably process with 2) and 3). Authentication stage the same and the corresponding values are the same, the Server thinks user legal and accept its request. Secondly, the Server receives HPW_{new} and $H(HPW_{new})$ instead of replacement $H(PWi)$, in the last return request success information to the Client. As showed in Fig.2.

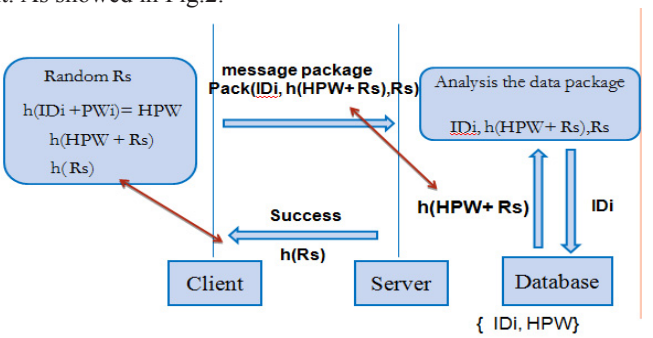

Fig.2 flow chart of Web security password authentication based the Single-block hash function

3.3 Improved the single-block hash function the authentication scheme

1) The scheme can withstand steal

Prove: If the attacker steals *Rs* and login message package, because of the one-way of H(.), according to *Rs* and $H(Rs + H(ID_i + PW_i))$, to get PW_i is difficult. If the attacker steals *Rs*, he has not the user password to fake $H(Rs + H(ID_i + PW_i))$. When the Server tests the data, he will be found out.

2) The scheme can withstand tamper with

Prove：If the attacker tempers with login message package, Pack≠Pack', and the Server checks Pack' and Pack0 computed by system, both are different, Pack0≠Pack'（Pack0≡Pack）,the authentication is failed. There is no threat to system and user. If the attacker tempers with *Rs* , the Client will receive *Rs*'(*Rs*'≠ *Rs*). Therefore $Pack(ID_i, H(Rs + H(ID_i + PW_i))) \neq Pack(ID_i, H(Rs' + H(ID_i + PW_i)))$. In a similar way, login failed will not be threatening to system and user badly.

3) The scheme can withstand replay

Prove：If the attackers steal to login message package, he can use the replay way to pretend to be the user, in this time two kind of situations: if the user has quit, the Server response to login request return of *Rs* is different at this time, the attacker can through the verification. If legal user does not quit, the replay news is effective. But in the Server the second step it will verify that the user has logged in online, thus to refuse the attacker's replay login.

4) Using mutual authentication can prevent the Server in replaying

From the above analysis, we can see that the Web user's identity authentication scheme in safety depends largely on the safety of H(.). Considering the cost, more use of the most common and mature MD5, SHA-1 and RIPEMD-160 . Evaluation H(.) safety standard is to look to find a pair of collision message how high the price. Cracking MD5 and SHA-1 main goal is to find a pair of collision or more messages.

4. The Experimental Results and Analysis

1) The general attack on MD5 basically has: the so-called direct attack that the attacker to find one plaintext M' is same as the original plaintext M, making H(M)=H(M′). H(M) is hash value of the plaintext

M.H(.) is the one-way hash function. The general attack is exhaustive possible proclaimed in writing to produce a and H(M) of the same hash results. The hash result of MD5 is 128 bits. If the attacker is using attempts per second article 10^8 expressly machine, need operation $2^{128}/(10^8*60*60*24*365)=1.79*10^{23}$days, about 10^{23}days. And the Single-Block hash function result is 128 bits ,too.

2) Birthday attack to MD5: the so-called birthday attack is to use probability to guide hash conflict discoveries, it is actually to find the two can produce the same hash result plaintext. If try to use 264 plaintexts, then they proclaimed in writing between at least one of the probability of conflict is 50%. If use a second try ten plaintext machine, average need to run 2/10*60*60*24*365=5.849 years, about six years to find one pair.

3) To MD5 differential attack: differential attack is through the comparative analysis of the difference between a specific expressly in through the encrypted change condition to attack the encryption system. It has proved that differential attack on the MD5 one cycle is effective, but to all four cycles is invalid. From the above analysis we can see that MD5 has higher security, so the paper presents the design of Web user's identity authentication scheme is safe and reliable.

5. Conclusion

The Web user's identity authentication at present mostly is used by MD5, but MD5 more suited to a long message, and the user's identity authentication password number is too low. So the paper designed an identity authentication based on the Single-Block hash function. from the experiment data we can see, the Single-Block hash function efficiency higher than MD5 algorithm, at the same time it can guarantee the security of the password authentication algorithm.

The algorithm overcomes the characteristics of the common the authentication scheme to achieve process based on insufficient, this paper puts forward a kind algorithm based on the Single-Block hash function, it meets the Web service user's identity authentication resistance to replay, steal, manipulation and common security threats, high efficiency, effectively solve the traditional account number-password scheme deficiency.

References

[1] Cheng Tian Fei Xin. The identity authentication technology and application of gossip. Computer Security, 2005,1
[2] Wan-dong Cai. Network and Information Security. Version 1. XiAn:The Northwest Industry University Press, 2004: 170~195
[3] Li-bo Dong. Research and Design in Password Authentication and Protection base on Web-servers. Huazhong University of Science & Technology Master's Thesis.2008:8~24
[4] Charles P.Pfleeger and Shari Lawrence Pfleeger. Security in Computing. Fourth Edition. Beijing: Electronic Industry Press.2007: 159~170
[5] He-sheng Wu, Tiao-li Fan, Wei-min Wu. An Efficient One-Time Password Authentication. Application Research Of Computers. 2003,23(5):45~47
[6] Xiang-dong Hu, Qin-fang Wei and Rong Hu. Applied Cryptograph. Version 2. Beijing: Electronic Industry Press. 2010: 188~221
[7] Zheng Hu. Network and Information Security. Beijing: Tsinghua University Press. 2006: 200~212
[8] Chin-Chen Chang and Ling-hua Wu. A New Password Authentication Scheme. Journal of Information Science and Engineering,1990,6(2):139~147
[9] William Stallings. Cryptography and Network Security: Principles and Practices, Fourth Edition. Beijing: Electronic Industry Press. 2007: 229~250